

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:

Toru KAMIWADA, et al.

Application No.:

Group Art Unit:

Filed: September 19, 2001

Examiner:

For: DEVICE CONTROL SYSTEM



**SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN
APPLICATION IN ACCORDANCE
WITH THE REQUIREMENTS OF 37 C.F.R. §1.55**

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

In accordance with the provisions of 37 C.F.R. §1.55, the applicant(s) submit(s) herewith a certified copy of the following foreign application:

Japanese Patent Application No. 2001-160083

Filed: May 29, 2001

It is respectfully requested that the applicant(s) be given the benefit of the foreign filing date(s) as evidenced by the certified papers attached hereto, in accordance with the requirements of 35 U.S.C. §119.

Respectfully submitted,

STAAS & HALSEY LLP

Date: September 19, 2001

By: 

James D. Halsey, Jr.
Registration No. 22,729

700 11th Street, N.W., Ste. 500
Washington, D.C. 20001
(202) 434-1500



日 本 国 特 許 庁
JAPAN PATENT OFFICE

Handwritten signature or initials.

11000 U.S. PTO
09/955945



別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2001年 5月29日

出 願 番 号

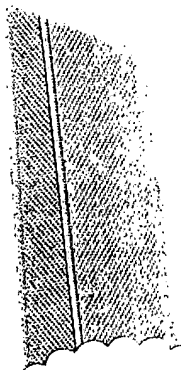
Application Number:

特願2001-160083

出 願 人

Applicant(s):

富士通株式会社

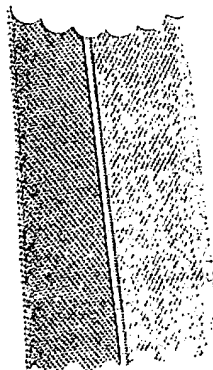
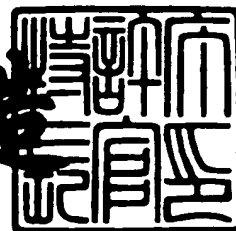


CERTIFIED COPY OF
PRIORITY DOCUMENT

2001年 8月10日

特許庁長官
Commissioner,
Japan Patent Office

及 川 耕 造



【書類名】 特許願

【整理番号】 0195025

【提出日】 平成13年 5月29日

【あて先】 特許庁長官 殿

【国際特許分類】 G06F 17/60

【発明の名称】 機器制御システム

【請求項の数】 5

【発明者】

 【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

 【氏名】 上和田 徹

【発明者】

 【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

 【氏名】 浅見 俊宏

【発明者】

 【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

 【氏名】 藤田 卓志

【特許出願人】

 【識別番号】 000005223

 【氏名又は名称】 富士通株式会社

【代理人】

 【識別番号】 100094145

 【弁理士】

 【氏名又は名称】 小野 由己男

 【連絡先】 06-6316-5533

【選任した代理人】

 【識別番号】 100094167

【弁理士】

【氏名又は名称】 宮川 良夫

【選任した代理人】

【識別番号】 100106367

【弁理士】

【氏名又は名称】 稲積 朋子

【手数料の表示】

【予納台帳番号】 020905

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9807456

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 機器制御システム

【特許請求の範囲】

【請求項 1】

有線または無線の宅内ネットワークを介して住宅内の 1 以上の機器に接続される機器制御サーバと、前記機器の操作に関する指示信号を有線または無線で送信可能な操作端末とを備える機器制御システムのアクセス制限方法であって、

前記操作端末に設定される固有の識別子を前記操作端末のアクセス権と関連付けるための端末情報の登録を受け付ける段階と、

前記操作端末の識別子と前記機器の操作に関する指示信号とを含む指示情報を受け付ける段階と、

前記指示情報に含まれる前記操作端末の識別子から前記操作端末のアクセス権を判定する段階と、

前記操作端末のアクセス権と前記機器に関する指示信号とに基づいて前記機器の制御を行う段階と、

を含む機器制御システムのアクセス制御方法。

【請求項 2】

請求項 1 に記載の機器制御システムのアクセス制御方法をコンピュータに実行させるためのプログラム。

【請求項 3】

請求項 2 に記載のプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項 4】

有線または無線の宅内ネットワークを介して住宅内の 1 以上の機器に接続され、操作端末から送信される前記機器の操作に関する指示信号に基づいて前記機器の制御を行う機器制御サーバであって、

前記操作端末に設定される固有の識別子を前記操作端末のアクセス権と関連付けるための端末情報の登録を受け付ける端末情報受付手段と、

前記操作端末の識別子と前記機器の操作に関する指示信号とを含む指示情報を

受け付ける指示情報受付手段と、

前記指示情報に基づいて前記操作端末のアクセス権を判定するアクセス権判別手段と、

前記アクセス権判別手段により判定された前記操作端末のアクセス権と前記指示情報に含まれる前記機器の操作に関する指示信号とに基づいて前記機器の制御を行う機器制御手段と、
を含む機器制御サーバ。

【請求項 5】

住宅内の 1 以上の機器と有線または無線の宅内ネットワークを介して接続される機器制御サーバを有する機器制御システムにおける前記機器の操作に関する指示信号を送信する操作端末であって、

固有の識別子を記憶する識別子記憶手段と、

前記機器制御サーバに前記識別子の登録を行う端末情報登録手段と、

前記の操作に関する指示入力を受け付ける入力受付手段と、

前記入力受付手段により受け付けた指示入力と、前記識別子記憶手段に記憶されている識別子とに基づいて指示情報を生成する指示情報生成手段と、

前記指示情報生成手段により生成された指示情報を無線または有線により送信する指示情報送信手段と、
を備える操作端末。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、家庭内のテレビやビデオなどの A V 機器、電話やパソコンなどの情報通信機器、エアコンや冷蔵庫などの家電機器について、家庭内および宅外からリモコンなどの操作端末を用いて動作制御を行ったり、ホームサーバ内に蓄積されている情報や、ホームサーバ経由で外部から取得できる情報を無線または有線の情報通信技術を介して利用するための機器制御システムに関する。

【0002】

【従来の技術】

家庭内の機器を遠隔操作するためのリモコンは、多くの場合には各機器と1対1で対応しており、このため複数の機器の操作を行うためには複数のリモコンが必要となる。これに対し、複数のリモコンが発信する信号を記憶させ、1つの操作端末で複数の機器を操作できるようにした統合型リモコンが提案されている。この統合型リモコンを用いた場合には、住宅内において各機器を制御することは可能であるが、宅外から各機器の制御を行うことが不可能である。

【0003】

家庭内のテレビやビデオなどのAV機器、電話やパソコンなどの情報通信機器、エアコンや冷蔵庫などの家電機器を宅内ネットワークで接続し、この宅内ネットワークに接続された機器制御サーバ（ホームサーバ）により各機器の制御を行うようにした機器制御システムの構成が考えられる。この場合、宅外からのアクセスには、ネットワークを介してホームサーバに接続することとなり、第3者からの不正なアクセスを防止するために、操作者の認証を行う必要性がでてくる。たとえば、各機器の操作を行うためのパスワードを設定しておき、機器の操作に関する指示を行う場合に操作端末からのパスワードの入力を受け付け、認証を行うことで第3者による不正なアクセスを防止することが可能となる。

【0004】

また、ホームサーバでは取得した各種情報を蓄積するための蓄積手段や宅外ネットワークを介して外部から取得可能な各種情報の提供を行うための外部接続手段などを備えている場合がある。このような各種情報を提供するためには、認証を行って利用者の特定を行う必要がある場合がでてくる。たとえば、未成年に見せることが好ましくないような映像コンテンツでは、その映像コンテンツを取り出してテレビに出力する前に、出力してもよいか否かの判定を行う必要となる。この場合も、利用者を特定するための認証情報としてパスワードの入力を要求し、利用者から入力されたパスワードが正当なものであるか否かを判断することにより、テレビなどの機器を制御してそのコンテンツの出力に関する制御を行うことが考えられる。

【0005】

各機器が設置されている住宅内からのアクセスである場合と宅外からのアクセ

スである場合を区別するために、各操作端末に異なるパスワードを設定することが考えられる。また、利用するコンテンツ毎やコンテンツの種別毎にパスワードを設定しておくことも可能である。このようにすることで1つのパスワードが第三者に知られてしまった場合であっても、その第三者によるアクセスが他の部分に影響することを抑制でき、不正なアクセスによる影響を最小限にとどめることができる。

【 0 0 0 6 】

【発明が解決しようとする課題】

前述したような機器制御システムにおいて、住宅内または宅外からホームサーバにアクセスを行う際にユーザの認証が必要となる場合、その都度パスワードの入力が必要となり作業が煩雑となる。また、このようなパスワード入力のみによる認証では、第三者にパスワードを知られてしまうとその者による不正なアクセスが可能となってしまう。

【 0 0 0 7 】

パスワードを定期的に変更することにより、不正なアクセスを抑制する効果があるが、完全に不正なアクセスを防止できるものではなく、パスワードを変更する手間がかかり、利用者にとって煩雑な作業が必要となるとともに、パスワードを忘れるという確率が高くなる。アクセス元となる操作端末毎に異なるパスワードを設定した場合やコンテンツやサービス毎にパスワードを設定した場合にも、利用者がそれぞれのパスワードを憶えておく必要があり、忘れてしまう確率も高くなる。

【 0 0 0 8 】

パスワードをリモコンやその他の操作端末に記憶させておき、パスワード入力の手間を省くことも考えられるが、このパスワードを第三者に知られてしまった場合に、不正なアクセスを防止することができない。特に、宅外からの不正なアクセスにより家庭内の情報が引き出されたり、改変された場合には、非常な不都合を生じるおそれがある。

【 0 0 0 9 】

本発明は、住宅内の機器を制御する機器制御システムにおいて、利用者の認証

作業の手間を軽減するとともに、第3者からの不正なアクセスを防止することを目的とする。

【0010】

【課題を解決するための手段】

本発明に係る機器制御システムのアクセス制限方法は、有線または無線の宅内ネットワークを介して住宅内の1以上の機器に接続される機器制御サーバと、機器の操作に関する指示信号を有線または無線で送信可能な操作端末とを備える機器制御システムのアクセス制限方法であって、操作端末に設定される固有の識別子を操作端末のアクセス権と関連付けるための端末情報の登録を受け付ける段階と、操作端末の識別子と機器の操作に関する指示信号とを含む指示情報を受け付ける段階と、指示情報に含まれる操作端末の識別子から操作端末のアクセス権を判定する段階と、操作端末のアクセス権と機器に関する指示信号とに基づいて機器の制御を行う段階とを含む。

【0011】

ここで、端末情報の登録を受け付ける際に操作端末に設定される公開鍵を受け付け、操作端末において秘密鍵で暗号化された所定のデータを受信し、公開鍵により復号化して所定のデータと照合することによって操作端末の認証を行う段階をさらに含む構成とすることができる。

【0012】

また、電子情報を取得するとともに蓄積手段内に蓄積する段階をさらに含み、機器に関する指示信号が蓄積手段に蓄積された電子情報へのアクセスを含む場合に、操作端末のアクセス権に基づいて電子情報の提供を許可するか否かを判断するように構成できる。

【0013】

さらに、機器の操作に関する指示信号が宅外ネットワークへのアクセスを含む場合に、操作端末のアクセス権に基づいて宅外ネットワークへのアクセスを許可するか否かを判断し機器の制御を行うように構成できる。この場合には、宅外ネットワーク上のコンテンツ毎にアクセスを許可するか否かを判断するように構成することも可能である。

【 0 0 1 4 】

また、操作端末からの指示情報を受信した際に、操作端末が宅内にあるか宅外にあるかを判別し、この判別結果と指示情報に含まれる操作端末の識別子から操作端末のアクセス権を判定するように構成できる。

【 0 0 1 5 】

さらに、操作端末を操作するユーザに関する情報を操作端末と関連付けるための個人情報の登録を受け付ける段階をさらに含み、指示情報に含まれる操作端末の識別子からこの操作端末に関連付けられた個人情報を抽出し、個人情報および端末情報からアクセス権を判定するように構成できる。

【 0 0 1 6 】

本発明では、上述したような機器制御システムのアクセス制御方法をコンピュータに実行させるためのプログラムを提案する。

また、本発明では、このような機器制御システムのアクセス制御方法をコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体を提案する。

【 0 0 1 7 】

本発明に係る機器制御サーバは、有線または無線の宅内ネットワークを介して住宅内の1以上の機器に接続され、操作端末から送信される機器の操作に関する指示信号に基づいて機器の制御を行う機器制御サーバであって、操作端末に設定される固有の識別子を操作端末のアクセス権と関連付けるための端末情報の登録を受け付ける端末情報受付手段と、操作端末の識別子と機器の操作に関する指示信号とを含む指示情報を受け付ける指示情報受付手段と、指示情報に基づいて操作端末のアクセス権を判定するアクセス権判別手段と、アクセス権判別手段により判定された操作端末のアクセス権と指示情報に含まれる機器の操作に関する指示信号とに基づいて機器の制御を行う機器制御手段とを含む。

【 0 0 1 8 】

ここで、端末情報の登録を受け付ける際に、操作端末に設定される公開鍵を受け付け、端末情報とともに端末情報記憶手段に格納する公開鍵受付手段と、所定のデータを送信し、操作端末において秘密鍵で暗号化された所定のデータを受信

し、公開鍵により復号化して所定のデータと照合することによって、操作端末の認証を行う操作端末認証手段とをさらに含む構成とすることができる。

【 0 0 1 9 】

また、端末情報受付手段は、端末情報の一部として操作端末の識別子と関連付けられる公開鍵の登録を受け付けるように構成できる。

さらに、電子情報を取得する電子情報取得手段と、電子情報取得手段により取得した電子情報を蓄積する電子情報蓄積手段とをさらに備え、機器に関する指示信号が電子情報蓄積手段に蓄積された電子情報へのアクセスを含む場合に、アクセス権判定手段は、操作端末のアクセス権を判定して電子情報の提供を許可するか否かを判断するように構成できる。

【 0 0 2 0 】

また、住宅外に存在する宅外ネットワークに接続可能な宅外通信手段をさらに備え、機器の操作に関する指示信号が宅外ネットワークへのアクセスを含む場合に、アクセス権判定手段は、操作端末のアクセス権を判定し宅外ネットワークへのアクセスを許可するか否かを判断するように構成できる。この場合、宅外ネットワーク上のコンテンツ毎にアクセスを許可するか否かを判断するように構成することも可能である。

【 0 0 2 1 】

さらに、指示情報受付手段により受け付けた指示情報に基づいて、操作端末が宅内にあるか宅外にあるかを判別する端末位置判別手段をさらに備え、アクセス権判定手段は、端末位置判別手段による判別結果に基づいて操作端末のアクセス権を判定するように構成できる。

【 0 0 2 2 】

また、操作端末を操作するユーザに関する情報を操作端末と関連付けるための個人情報の登録を受け付ける個人情報受付手段をさらに含み、アクセス権判定手段は、指示情報に含まれる操作端末の識別子からこの操作端末に関連付けられた個人情報を抽出し、個人情報および前記端末情報からアクセス権を判定するように構成できる。

【 0 0 2 3 】

本発明に係る操作端末は、住宅内の1以上の機器と有線または無線の宅内ネットワークを介して接続される機器制御サーバを有する機器制御システムにおける機器の操作に関する指示信号を送信する操作端末であって、固有の識別子を記憶する識別子記憶手段と、識別子を機器制御サーバに登録する端末情報登録手段と、機器の操作に関する指示入力を受け付ける入力受付手段と、入力受付手段により受け付けた指示入力と識別子記憶手段に記憶されている識別子とに基づいて指示情報を生成する指示情報生成手段と、指示情報生成手段により生成された指示情報を無線または有線により送信する指示情報送信手段とを備える。

【0024】

ここで、現在の位置情報を取得する位置情報取得手段をさらに備え、指示情報生成手段は、指示入力、識別子および位置情報取得手段により取得した位置情報に基づいて指示情報を生成するように構成できる。

【0025】

また、操作するユーザに関する情報の入力を受け付ける個人情報入力手段をさらに備え、指示情報生成手段は、指示入力、識別子および個人情報入力手段により受け付けたユーザに関する情報に基づいて指示情報を生成するように構成できる。

【0026】

さらに、指示情報を暗号化するための暗号鍵を格納する暗号鍵記憶手段をさらに備え、指示情報生成手段は、暗号鍵記憶手段に記憶されている暗号鍵により指示入力と識別子を暗号化して指示情報を生成するように構成できる。

【0027】

また、秘密鍵を記憶する秘密鍵記憶手段と、秘密鍵に対応する公開鍵を記憶する公開鍵記憶手段と、秘密鍵によりデータを暗号化する暗号化処理手段とをさらに含み、端末情報登録手段により機器制御サーバに端末情報の登録を行う際に公開鍵を機器制御サーバに送信し、指示情報を送信する際に、機器制御サーバから受信する所定のデータを秘密鍵によって暗号化して認証情報として送信する構成とすることが可能である。

【0028】

【発明の実施の形態】

〈概略構成〉

本発明の 1 実施形態が採用される機器制御システムの概略構成を図 1 に示す。

【0029】

住宅内に設置されるテレビ 5 1 やビデオ 5 2 などの A V 機器、パソコン 5 3 や電話機 5 4 などの情報通信機器、エアコン 5 5 や冷蔵庫 5 6 などの家電機器などは、宅内ネットワーク 5 によってホームサーバ 1 に接続されている。宅内ネットワーク 5 は、有線または無線で構成することが可能であり、たとえば、E t h e r n e t や電灯線 L A N などの有線による L A N、B l u e t o o t h、H o m e R F、I E E E 8 0 2 . 1 1 B などの電波を用いた無線通信手段や I r D A などの赤外線を用いた無線通信手段などによる無線による L A N などを採用し得る。

【0030】

テレビ 5 1、ビデオ 5 2、パソコン 5 3、電話機 5 4、エアコン 5 5、冷蔵庫 5 6 などの機器は、リモコン 3 による操作が可能となっている。このリモコン 3 は、たとえば、機器の操作に関する指示入力を受け付けるための操作ボタン、受け付けた指示入力に基づいて指示情報を送信するとともに機器などからのデータを受信するための赤外線送受信手段、受け付けた操作内容や機器などから受信したデータを表示するための表示手段などを備えるものである。リモコン 3 は、各機器に指示情報を送信するように構成することも可能であり、また、ホームサーバ 1 に指示情報を送信するように構成することも可能である。

【0031】

ホームサーバ 1 は、地上波受信用アンテナ、衛星放送受信用アンテナまたは C A T V のケーブル接続部などの放送受信手段 8 を介して、画像情報、音声情報および文字情報などを受信することが可能となっており、受信した情報をテレビ 5 1 やビデオ 5 2 を介してユーザに提供することが可能となっている。

【0032】

また、ホームサーバ 1 は、電話回線網やインターネット網などの宅外ネットワーク 7 と接続されており、パソコン 5 3 や電話機 5 4 から外部とのデータの送受

信を行うことを可能とする。

【0033】

ホームサーバ1は、たとえば図2に示すような構成となっている。

ホームサーバ1は、各種情報を受け付けるための操作パネル11を備えている。この操作パネル11は、有線または無線で接続されたキーボードや操作ボタンなどで構成することが可能であり、ホームサーバにCRTや液晶表示パネルなどを備えている場合には、マウスやトラックボールなどのポインティングデバイスで構成することも可能である。操作パネル11から入力された各種情報は、入力処理部12によって受け付けられ、通信制御部15により対応する部分に送信される。

【0034】

また、ホームサーバ1は、宅内ネットワーク5と接続される宅内通信部13を備えている。この宅内通信部13は、宅内ネットワーク5とデータの送信を行うものであり、前述したようなEthernetや電灯線LANなどの有線によるLAN、Bluetooth、HomeRF、IEEE802.11Bなどの電波を用いた無線通信手段やIrDAなどの赤外線を用いた無線通信手段などによる無線によるLANに対応するインターフェイスで構成することができる。

【0035】

さらにホームサーバ1は、宅外ネットワーク7と接続される宅外通信部14を備えている。この宅外通信部14は、電話通信網やインターネット網に接続するためのルータやモデムなどで構成することができる。

【0036】

また、ホームサーバ1は、放送受信手段8によって受信される画像情報、音声情報、文字情報などの情報を受け付ける放送受信部21を備えている。放送受信部21は、受信した情報を蓄積情報データベース23に蓄積するか否かを管理する蓄積情報管理部22に接続されている。蓄積情報データベース23は、ハードディスクドライブやMO、CD-R、CD-RW、DVDなどの記録メディアを用いたデータ格納手段で構成することが可能である。

【0037】

入力処理部 12、宅内通信部 13、宅外通信部 14、蓄積情報管理部 22は通信制御部 15に接続されている。通信制御部 15は、さらにアクセス権制御部 16に接続されている。アクセス権制御部 16は、端末情報管理部 17と個人情報管理部 18に接続されている。

【0038】

端末情報管理部 17は、リモコン 3や操作パネル 11などから入力される端末情報に基づいて端末情報データベース 19を更新するとともに、アクセス権制御部 16からの要求に応じて端末情報データベース 19の内容を読み出して端末情報を提供するものである。

【0039】

個人情報管理部 18は、リモコン 3や操作パネル 11などから入力される個人情報に基づいて個人情報データベース 20を更新するとともに、アクセス権制御部 16からの要求に基づいて個人情報データベース 20の内容を読み出して個人情報を提供するものである。

【0040】

通信制御部 15は、ユーザや各機器から送信されてくる指示情報に基づいて、各機器から送出される情報、宅外通信部 14で受信した情報、放送受信部 21で受信した情報、蓄積情報データ 23内の蓄積情報などを指示情報に対応する機器などに送信してユーザに提供し、リモコン 3などの操作端末に関する端末情報や操作端末を使用するユーザの個人情報などの登録情報を受信した場合に、端末情報管理部 17および個人情報管理部 18に送信して各情報の登録を行わせるものである。

【0041】

リモコン 3の概略構成を図 3に示す。

リモコン 3は、ユーザからの指示入力を受け付けるための入力装置 39を備えている。入力装置 39は、通常の押しボタンスイッチなどで構成されるものであり、液晶表示パネル上に透明電極が重ねて配置されたタッチパネルで構成することも可能である。

【0042】

リモコン 3 は、ユーザから受け付けた指示入力の内容や現在のリモコンの動作モード、各機器の動作モード、その他の情報を表示するための表示装置 4 0 を備えている。表示装置 4 0 は、液晶表示パネルや L E D、E L など表示デバイスを採用することが可能である。

【 0 0 4 3 】

また、リモコン 3 は、各機器またはホームサーバ 1 と通信可能な通信装置 4 1 が設けられている。通信装置 4 1 は、I r D A などの赤外線通信プロトコルを用いた通信手段が採用され、また、B l u e t o o t h、H o m e R F、I E E E 8 0 2 . 1 1 B などの電波を用いた通信手段を用いることも可能で、さらに有線により機器またはホームサーバ 1 に接続された構成とすることも可能である。

【 0 0 4 4 】

リモコン 3 の内部には、各部を制御するための中央制御部 3 4 を備えている。この中央制御部 3 4 には、入力処理部 3 1、表示処理部 3 2、通信処理部 3 3、端末 I D 記憶部 3 5、公開鍵記憶部 3 6、暗号化処理部 3 7 などが接続されている。

【 0 0 4 5 】

入力処理部 3 1 は、入力装置 3 9 から入力されるユーザの指示入力を受け付ける。表示処理部 3 2 は、入力装置 3 9 から入力された指示入力の内容やリモコン 3 の動作モードや各機器の動作モード、その他の情報を表示装置 4 0 に送信してこれを表示させるものである。通信処理部 3 3 は、ユーザから入力された指示入力に基づく指示情報を各機器またはホームサーバ 1 に送信するとともに、各機器の動作モードや動作状態に関する情報を受信して中央制御部 3 4 に送信する。

【 0 0 4 6 】

端末 I D 記憶部 3 5 は、リモコン 3 に設定される固有の識別子を記憶するものであり、予め設定された製品 I D や設定権を有する者が入力装置 3 9 などから入力した固有 I D を格納する。この端末 I D 記憶部 3 5 は、ROM、E E P R O M、電源バックアップされた R A M などの記憶デバイスで構成することが可能である。

【 0 0 4 7 】

公開鍵記憶部 36 は、操作端末毎に設定され指示情報の送信先であるホームサーバ 1 などに予め送信しておく公開鍵を格納しておくものである。この公開鍵記憶部 36 は、ROM、EEPROM、電源バックアップされた RAM などの記憶デバイスで構成することが可能である。

【0048】

暗号化処理部 37 は、秘密鍵記憶部 38 に格納されている暗号鍵に基づいて、送信する指示情報を暗号化するものであり、秘密鍵記憶部 38 とともに IC チップ化された論理演算回路で構成することができる。

【0049】

〈登録処理〉

リモコン 3 を各機器の操作端末として登録する場合の動作を説明する。

ホームサーバ 1 における登録処理のフローチャートを図 4 に示す。

【0050】

ホームサーバ 1 は、ステップ S11 において、宅内通信部 13 を介して端末情報を受信し、この端末情報を通信制御部 15、アクセス権制御部 16、端末情報管理部 17 を介して端末情報データベースに格納するための登録受付状態に設定する。ステップ S12 では、登録受付状態の開始時刻 t_0 に現在時刻を代入する。

【0051】

ステップ S13 では、操作端末から登録要求があったか否かを判別する。リモコン 3 から登録要求を受信した場合にはステップ S17 に移行し、リモコン 3 からの登録要求がない場合にはステップ S14 に移行する。

【0052】

ステップ S14 では、登録中止ボタンが入力されたか否かを判別する。リモコン 3 から登録中止の指示入力を受け付けた場合にはステップ S16 に移行し、登録中止の指示入力がない場合にはステップ S15 に移行する。

ステップ S15 では、時刻 t_0 からの経過時間が所定時間 t_{MAX} 以上となったか否かを判別する。登録受付状態の開始から所定時間 t_{MAX} が経過した判断した場合にはステップ S16 に移行し、そうでない場合にはステップ S13 に移行する。

【0053】

ステップS16では、登録受付状態を解除して処理を終了する。

ステップS17では、登録受付状態の解除を行う。ここでは、登録要求を送信してきたリモコン3に対して登録要求受理信号を送信し、他の操作端末からの新たな登録要求を禁止する。

【0054】

ステップS18では、操作端末から端末IDと公開鍵を受信する。ここでは、リモコン3の端末ID記憶部35に格納されているリモコン3の識別子と、公開鍵記憶部36に格納されている公開鍵を受信する。この場合、リモコン3から送信される端末IDと公開鍵の情報を、宅内ネットワーク5に接続された各機器のうちのいずれかで受信し、これをホームサーバ1の宅内通信部14に送信させるように構成することもでき、また、ホームサーバ1により直接リモコン3からの情報を受信するように構成することもできる。

【0055】

ステップS19では、受信した操作端末の端末IDおよび公開鍵を記録する。ここでは、リモコン3に設定された固有の識別子と公開鍵を端末情報データベース19内に格納する。

【0056】

登録処理時のリモコン3における動作を図5のフローチャートに示す。

ステップS21では、登録要求を送信する。ここでは、通信装置41を用いて宅内ネットワーク5に接続されている機器のうちのいずれかまたはホームサーバ1に直接登録要求信号を送信する。

【0057】

ステップS22では、登録要求が受理されたか否かを判別する。ホームサーバ1から送出される登録要求受理信号を受信した場合には、ステップS23に移行する。

【0058】

ステップS23では、端末IDと公開鍵の送信を行う。ここでは、端末ID記

憶部 3 5 に格納されているリモコン 3 に固有の識別子および公開鍵記憶部 3 6 に格納されている公開鍵を読み出して、通信装置 4 1 を介して送信する。

【 0 0 5 9 】

〈操作端末の認証〉

操作端末を用いてホームサーバにアクセスする際の、操作端末の認証の手順を説明する。

【 0 0 6 0 】

操作端末からのアクセスを受け付ける際に、ホームサーバ 1 が行う操作端末の認証の動作を図 6 のフローチャートを用いて説明する。

ステップ S 3 1 では、操作端末の端末 I D を受け付ける。ここでは、リモコン 3 から送信される端末 I D を宅内通信部 1 3 などを経由して受信してこれを受け付ける。

【 0 0 6 1 】

ステップ S 3 2 では、登録されている端末情報から、送信されてきた端末 I D に対応する端末情報を取り出す。ここでは、端末情報データベース 1 9 内を検索して、受信した端末 I D に対応する端末情報を抽出する。

【 0 0 6 2 】

ステップ S 3 3 では、受信した端末 I D が登録されている操作端末であるか否かを判別する。端末情報データベース 1 9 に登録されていない端末 I D である場合には、認証失敗のエラーメッセージを操作端末に送信し処理を終了する。また、端末情報データベース 1 9 に端末 I D が存在する場合にはステップ S 3 4 に移行する。

【 0 0 6 3 】

ステップ S 3 4 では、認証用データ列 A を生成する。ここでは、認証用データとして所定の方法でデータ列 A を生成する。ステップ S 3 5 では、認証用データ列 A を操作端末に送信する。ステップ S 3 6 では、操作端末で暗号化されたデータ列 B を受信する。このデータ列 B は、送信した認証用データ A を操作端末側において秘密鍵によって暗号化したものである。ステップ S 3 7 では、受信したデータ列 B を操作端末に対応する公開鍵で復号化する。ここでは、端末情報データ

ベース19から抽出した端末情報に含まれる公開鍵を用いて、データ列Bを復号化する。

【0064】

ステップS38では、復号化したデータがデータ列Aと一致するか否かを判別する。リモコン3の秘密鍵記憶部38に格納されている秘密鍵で暗号化されたデータは、対応する公開鍵でのみ復号できるように構成されており、秘密鍵で暗号化されたデータ列Bを送信してきた操作端末が正当な操作端末であれば、公開鍵で復号化されたデータが元の認証用データ列Aと一致するはずである。復号化されたデータ列が認証用データ列Aと一致した場合には認証成功した旨のメッセージを送信し、機器の操作に関する指示情報を受け付ける。また、復号化されたデータ列が認証用データ列Aと一致しない場合には、認証失敗のエラーメッセージを操作端末に送信し処理を終了する。

【0065】

リモコン3からアクセスを行う際の操作端末認証時の動作を図7のフローチャートを用いて説明する。

ステップS41では、ホームサーバ1から送信されてくる認証用のデータ列Aを受信する。ステップS42では、受け取った認証用のデータ列Aを秘密鍵で暗号化する。ここでは、秘密鍵記憶部38に格納されている秘密鍵を用いて暗号化処理部37がデータ列Aを暗号化して暗号化データ列Bを生成する。秘密鍵記憶部38に格納されている秘密鍵は、外部からの読み出しができないように構成されており、暗号化処理部37による暗号化にのみ用いられるように構成されている。

【0066】

ステップS43では、暗号化したデータ列Bをホームサーバ1に送信する。ここでは、通信装置41を用いて宅内ネットワーク5に接続されている機器のうちいずれか、またはホームサーバ1に直接送信する。

【0067】

ステップS44では、認証に成功したか否かを判別する。ホームサーバ1から認証に成功した旨のメッセージを受信した場合には次の処理に移行する。ホーム

サーバ1から認証に失敗した旨のメッセージを受信した場合には、認証失敗のメッセージを表示装置40に表示して処理を終了する。

【0068】

〈操作制御〉

実際にリモコン3から各機器の指示情報を送信して操作する場合の例を説明する。

【0069】

ホームサーバ1では、放送受信部21を介して受信した動画像データを蓄積情報データベース23に格納することが可能となっている。この蓄積情報データベース23に蓄積されている動画像データをリモコン3から操作してテレビ51に表示させる場合について説明する。テレビ51は、リモコン3によりチャンネル選択やメニュー選択などの操作を行うことが可能となっており、宅内ネットワーク5を介してホームサーバ1と接続されている。

【0070】

リモコン3によりテレビのメニューを選択し、ホームサーバ1にある情報の一覧を表示するように要求する。このメニュー選択を受けて、テレビ51はホームサーバ1と通信を行い、蓄積情報データベース23内に蓄積されている情報の一覧情報を要求する。この一覧情報の要求時に、指示情報が送信されたリモコン3の端末IDも併せて送信する。

【0071】

一覧情報の要求を受けたホームサーバ1は、受け取った端末IDを元に操作端末の認証処理を実行する。前述したように、認証用の文字列Aを生成してこれを送信して、秘密鍵で暗号化された文字列Bを受信し、これを公開鍵で復号化して文字列Aと照合することによって、操作端末の認証を行うことができる。操作端末の認証に成功した場合には、蓄積情報データベース23内に蓄積されている情報の一覧を送信する。

【0072】

テレビ51では、ホームサーバ1から送信されてきた一覧情報を表示し、ユーザに見たい動画像データの選択を行わせる。この動画像データの選択についても

、リモコン3の操作により送信される指示情報をテレビ51により受け付けて、宅内ネットワーク5を介してホームサーバ1に送信するように構成する。

【0073】

ホームサーバ1は、動画像データの選択要求についても操作端末の認証を行って、認証に成功した場合についてのみ、その動画像データをテレビ51に送出し、表示させるように構成される。

【0074】

〈宅外からのアクセス〉

前述した例では操作端末を宅内で使用される統合型リモコンとしているが、これに代えて宅外からホームサーバ1にアクセスして各機器の操作に関する指示を行うように構成することが考えられる。たとえば、各機器が設置されている住宅外のパソコンや電話機などを利用してインターネット網や電話回線網などを通じて操作の指示を行う場合が考えられる。また、携帯電話やPHS、PDA(Personal Digital Assistants)などの携帯端末から無線電話網を介して機器操作の指示を行う場合が考えられる。これら操作端末は前述のリモコン3とほぼ同様の構成であり、通信装置41がそれぞれの通信手段に対応するインターフェイスで構成される。このような場合も、前述と同様にして、パソコン、電話機、携帯電話、PHS、PDAなどの端末IDを予めホームサーバ1に登録しておき、同時に各操作端末の認証処理に用いるための公開鍵をホームサーバ1に登録しておく。電話機や携帯電話、PHSなどの場合には、端末IDとしてその電話番号を登録するように構成することも可能である。このような操作端末を用いて宅外からアクセスして各機器の操作を行う場合を説明する。ここで、エアコン55の設定温度を調節する場合を例として説明する。

【0075】

まず、操作端末から宅内ネットワーク5を介してホームサーバ1にアクセスし、操作端末の端末IDを送信するとともにエアコン55の現在の状態に関する情報を要求する要求信号を送信する。ホームサーバ1は、図6に示すような操作端末の認証処理を実行し、認証に成功した場合には、宅内ネットワーク5を介してエアコン55の現在の状態に関する情報を取得し、この情報を操作端末に送信す

る。

【0076】

ユーザは、操作端末の表示装置40に表示されるエアコン55の現在の状態に関する情報を参照し、エアコン55の電源投入、運転モード変更、設定温度変更などの必要な指示情報を入力する。操作端末では、ユーザから入力された指示情報を操作端末の端末IDとともにホームサーバ1に送信する。

【0077】

ホームサーバ1はこの指示情報を受信すると、端末IDに基づく端末情報に基づいて再度操作端末の認証処理を実行する。ここで認証に成功した場合には、指示情報に基づいて、エアコン55の操作に関する制御信号を生成して、エアコン55の制御を実行する。

【0078】

このように、操作端末からの指示情報を受信する度に認証処理を行うことにより、第3者からの不正なアクセスを防止することができ、住宅内の各機器を安全に操作することが可能となる。また、ユーザが操作端末の端末IDを意識することなく、ホームサーバ1における操作端末の認証処理が行われるため、ユーザがパスワードなどを記憶しておく必要がなく、第3者にパスワードが漏洩して不正に使用されることを防止できる。

【0079】

操作端末とホームサーバ1との間の通信において、データを暗号化して送受信するように構成することも可能である。この場合、電話回線網やインターネット網、携帯電話網などの通信経路上において第3者に通信をモニタされた場合であっても、その内容を知られることが防止できる。ここでの暗号化方法は、公開鍵暗号を用いることが可能である。

【0080】

〈個人情報に基づくアクセス制限〉

ホームサーバ1において、操作端末を操作するユーザの個人情報を管理し、この個人情報に基づいてアクセス制限を行うように構成することができる。たとえば、1つのリモコン3につき1個人を対応付けて個人情報を登録し、この個人情報

報に基づいてそのリモコン3からの操作に対する制限を設けることが可能となる。

【0081】

リモコン3を操作するユーザの個人情報をホームサーバ1に登録する際の手順を図8のフローチャートを用いて説明する。

リモコン3からユーザの個人情報の登録要求があった場合、ステップS51において登録要求のあった操作端末の端末情報を呼び出す。ここでは、端末情報データベース19から該当する端末IDの端末情報を呼び出す。

【0082】

ステップS52では、登録要求があった操作端末の端末情報が登録済みであるかを判別する。登録要求があった操作端末の端末情報が端末情報データベース19に登録されていると判断した場合にはステップS53に移行し、そうでない場合にはエラーメッセージを送信する処理を終了する。

【0083】

ステップS53では、操作端末から個人名を受信する。ホームサーバ1はリモコン3に対して個人名を入力を促す入力要求を送信し、これに対応してユーザが入力した個人名データをリモコン3から受信する。

【0084】

ステップS54では、操作端末から個人情報を受信する。ホームサーバ1はリモコン3に対して個人情報の入力进行を促す入力要求を送信し、これに対してユーザが入力した個人情報のデータをリモコン3から受信する。ここで、ユーザから入力される個人情報として、たとえば、年齢、性別などの基本データの他に、会員制のサービスを利用する場合のそのサービスに対するパスワードなどを登録することができる。また、クレジットによる買い物やオンラインショッピングなどを利用する際に必要となる住所、電話番号、クレジットカード番号などを登録しておくことも可能である。さらに、リモコン3を使用するユーザの認証を行うために、指紋情報、虹彩情報、網膜情報、声紋情報などの生体情報を登録しておくことも可能である。

【0085】

ステップS55では、受信した個人名が登録済みであるか否かを判断するために、個人情報データベース20の情報を読み出す。ステップS56では、受信した個人名が登録されているか否かを判断する。受信した個人名が個人情報データベース20に登録されていると判断した場合にはステップS58に移行し、そうでないと判断した場合にはステップS57に移行する。

【0086】

ステップS57では、受信した個人情報を新規に登録する。ここでは、受信した個人情報のレコードを個人情報データベース20内に新たに作成して格納する。ステップS58では、受信した個人情報に基づいて、個人情報データベース20内の該当するレコードの内容を更新する。

【0087】

ステップS59では、操作端末に対応する個人名を記録する。登録要求があったリモコン3と登録された個人情報を関連付けるために、端末情報データベース19の該当する端末情報に個人名を関連付けて登録する。

【0088】

このように操作端末を操作するユーザの個人情報に関連付けて登録しておくことによって、個人情報に基づくアクセス制限を行うことが可能となる。ホームサーバ1の蓄積情報データベース23内に蓄積された情報へのアクセス、CATVや衛星放送の利用について、個人に対するアクセス制限を設定している場合には、操作端末からアクセス要求があった場合に、操作端末の認証を行った後、その操作端末に関連付けられた個人情報を読み出して、操作しているユーザのアクセス権を判定し、アクセスを許可するか否かを決定することができる。

【0089】

たとえば、操作端末から蓄積情報データベース20内の情報へのアクセス要求があった場合、ホームサーバ1は要求のあった操作端末の認証処理を実行し、操作端末の認証に成功した場合に、その操作端末に関連付けられた個人情報を個人情報データベース20から取り出し、要求された情報へのアクセス権を判定してアクセスを許可するか否かを決定する。このことにより、未成年に好ましくないとされる映画や画像データなどが蓄積情報データベース23に蓄積されているよ

うな場合に、操作端末からのその情報へのアクセス要求があると、ホームサーバ1は端末情報データベース19からその操作端末に対応する個人名を特定し、この個人名から個人情報データベース20内の個人情報を取得して、その情報へのアクセス権を判定する。アクセス要求のあった情報が18歳以上の者にのみアクセス許可するように設定されており、アクセス要求があった操作端末に対応するユーザの個人情報が18歳未満である場合には、情報へのアクセス要求を拒否する。このような蓄積情報データベース23に蓄積されている情報のアクセス要求は、テレビ51への表示を要求する場合が考えられるが、アクセス要求を拒否する場合には、この情報へのアクセス権がない旨のメッセージをテレビ51の画面またはスピーカーに出力してユーザに知らせるように構成できる。

【0090】

個人情報の登録および変更については、各操作端末にマスタパスワードを設定しておき、正当なマスタパスワードが入力されたときのみ、実行することが可能であるような構成とすることができる。このことにより、第3者が不正使用を目的として個人情報を改竄することを防止することができる。

【0091】

〈宅外へのデータ送出〉

宅外において買い物を行う場合には、個人情報データベース20にクレジットカード番号を予め記憶させておき、登録された操作端末を用いてホームサーバ1を介してクレジット会社と通信を行い、支払の手続きを行うことが考えられる。この場合、ホームサーバ1が宅外ネットワーク7を介してクレジット会社とのデータ通信を行い、クレジットカード番号などの必要事項を送信するため、買い物をした店にクレジットカード番号を知られることがなく、安全に決済を行うことが可能となる。

【0092】

CATV、衛星放送などの双方向通信やパソコン53からインターネットを通じてのオンラインショッピングを行う場合にも、住所、電話番号、クレジットカード番号などを個人情報として登録しておくことにより、この登録情報を用いて簡単にデータ送信を行うことが可能となり、ユーザの手間を省くことが可能とな

る。このような個人情報は、登録されていない操作端末を用いて見ることはできないため、第3者に情報が漏洩することを防止できる。

【0093】

また、会員制の有料コンテンツに宅外からアクセスする場合に、個人情報データベース20にその有料コンテンツにアクセスするためのパスワードを予め登録しておき、ホームサーバ1によりその有料コンテンツの提供者との通信を行い、有料コンテンツを利用するように構成できる。この場合、ユーザが、各有料コンテンツの提供者毎のパスワードやサービス毎に設定されているパスワードをすべて記憶しておく必要がなく、パスワードが第3者に漏洩することも防止できる。

【0094】

〈端末情報および個人情報によるアクセス制限〉

端末情報によるアクセス制限と操作端末に関連付けられたユーザの個人情報によるアクセス制限とを統合して、ホームサーバ1に対するアクセス制限を行う場合について、図9のフローチャートに基づいて説明する。ここでも、蓄積情報データベース23に蓄積されている情報へのアクセス要求があった場合について説明する。

【0095】

操作端末から蓄積情報データベース23に蓄積されている情報へのアクセス要求があった場合には、ステップS61において要求された情報の種類についてのデータを蓄積情報データベース23から取得する。ステップS62では、要求された情報に対してアクセス制限が設定されているか否かを判別する。蓄積情報データベース23に蓄積された情報には、その情報毎にアクセス制限が設定されている場合と、分類された種類毎にアクセス制限が設定されている場合が考えられる。いずれの場合であっても、アクセス要求があった情報に対してアクセス制限が設定されていないと判断した場合にはステップS63に移行し、アクセス制限が設定されている場合にはステップS64に移行する。

【0096】

ステップS63では、宅内からのアクセスであるか否かを判別する。アクセス要求を送信してきた操作端末の端末IDから端末情報を取得し、宅内に存在する

操作端末であるか否かを判断し、宅内からのアクセスではないと判断した場合にはこの操作端末からのアクセスを拒否し、蓄積情報データベース23内に蓄積された該当する情報の提供を行わない。また、宅内からのアクセスであると判断した場合には、この操作端末からのアクセスを許可し、蓄積情報データベース23内の該当する情報の提供を行う。この場合、アクセス制限が設定されていない情報を宅外からアクセスすることを拒否するように設定しているが、宅外からのアクセスを許可するように構成することも可能である。

【0097】

ステップS64では、操作端末の認証を行う。前述したように、認証用データ列を送信し、操作端末において秘密鍵で暗号化されたデータ列を受信し、公開鍵を用いて復号化して元の認証用データ列と照合することにより、登録されている正当な操作端末であるか否かの判断を行う。操作端末の認証に失敗した場合には、アクセスを拒否する旨のメッセージを操作端末に送信しこの処理を終了する。操作端末の認証に成功した場合には、ステップS66に移行する。

【0098】

ステップS66では、個人情報に基づくアクセス制限が設定されているか否かを判別する。アクセス要求があった情報に個人情報によるアクセス制限が設定されていない場合には、操作端末からのアクセス要求を許可する。また、アクセス要求があった情報に個人情報によるアクセス制限が設定されている場合には、ステップS67に移行する。

【0099】

ステップS67では、アクセス要求を送信してきた操作端末の端末IDに基づいて端末情報データベース19から対応する端末情報を取得し、これから関連付けられているユーザの個人名を特定し、個人情報データベース20から該当するユーザの個人情報を取得する。

【0100】

ステップS68では、取得した個人情報が情報へのアクセス制限を満たしているか否かを判別する。アクセス要求を送信してきた操作端末に関連付けられたユーザの個人情報が、アクセス要求があった情報に設定されているアクセス制限を

満たしていないと判断した場合には、操作端末に対してアクセスを拒否する旨のメッセージを送信しこの処理を終了する。また、アクセス要求を送信してきた操作端末に関連付けられたユーザの個人情報が、アクセス要求があった情報に設定されているアクセス制限を満たしていると判断した場合には、操作端末に対してこの情報の提供を行う。

【0101】

このように、アクセス要求を行った操作端末が宅内にあるものか否かの情報、操作端末の端末情報や操作端末に関連付けられたユーザの個人情報などに基づいてアクセス制限を行うことによって、ユーザによる認証処理の手間を軽減し、利便性を保ったままで、第3者による不正なアクセスを防止して、家庭内の情報を保護することが可能となる。

【0102】

操作端末を紛失した場合であっても、ホームサーバ1の端末情報データベース19からその操作端末の情報を末梢することにより、個人情報の記録を削除することなくその操作端末を用いて第3者が不正にアクセスすることを防止できる。

【0103】

〈他の実施形態〉

操作端末として携帯電話やPHSなどを用いる場合には、宅内、宅外ともに同一の操作端末で指示情報を送信することが可能となる。この場合、携帯電話やPHSなどのサービス提供会社により提供されている位置情報提供サービスを利用して、操作端末の位置を取得し、これにより宅内であるか宅外であるかの判定を行うように構成することも可能である。

(付記1)

有線または無線の宅内ネットワークを介して住宅内の1以上の機器に接続される機器制御サーバと、前記機器の操作に関する指示信号を有線または無線で送信可能な操作端末とを備える機器制御システムのアクセス制限方法であって、

前記操作端末に設定される固有の識別子を前記操作端末のアクセス権と関連付けるための端末情報の登録を受け付ける段階と、

前記操作端末の識別子と前記機器の操作に関する指示信号とを含む指示情報を受け付ける段階と、

前記指示情報に含まれる前記操作端末の識別子から前記操作端末のアクセス権を判定する段階と、

前記操作端末のアクセス権と前記機器に関する指示信号とに基づいて前記機器の制御を行う段階と、

を含む機器制御システムのアクセス制御方法。

【 0 1 0 4 】

(付記 2)

前記端末情報の登録を受け付ける際に前記操作端末に設定される公開鍵を受け付け、

前記操作端末において秘密鍵で暗号化された所定のデータを受信し、前記公開鍵により復号化して前記所定のデータと照合することによって前記操作端末の認証を行う段階をさらに含む付記 1 に記載の機器制御システムのアクセス制御方法。

【 0 1 0 5 】

(付記 3)

前記公開鍵は、前記端末情報の一部として前記操作端末の識別子と関連付けられて登録される、付記 2 に記載の機器制御システムのアクセス制御方法。

【 0 1 0 6 】

(付記 4)

電子情報を取得するとともに蓄積手段内に蓄積する段階をさらに含み、

前記機器に関する指示信号が前記蓄積手段に蓄積された電子情報へのアクセスを含む場合に、前記操作端末のアクセス権に基づいて前記電子情報の提供を許可するか否かを判断する、付記 1 ～ 3 のいずれかに記載の機器制御システムのアクセス制御方法。

【 0 1 0 7 】

(付記 5)

前記機器の操作に関する指示信号が宅外ネットワークへのアクセスを含む場合

に、前記操作端末のアクセス権に基づいて前記宅外ネットワークへのアクセスを許可するか否かを判断し前記機器の制御を行う、付記1～4のいずれかに記載の機器制御システムのアクセス制御方法。

【0108】

(付記6)

前記宅外ネットワーク上のコンテンツ毎にアクセスを許可するか否かを判断する、付記5に記載の機器制御システムのアクセス制御方法。

【0109】

(付記7)

前記操作端末からの指示情報を受信した際に、前記操作端末が宅内にあるか宅外にあるかを判別し、この判別結果と前記指示情報に含まれる前記操作端末の識別子から前記操作端末のアクセス権を判定する、付記1～6のいずれかに記載の機器制御システムのアクセス制御方法。

【0110】

(付記8)

前記操作端末を操作するユーザに関する情報を前記操作端末と関連付けるための個人情報の登録を受け付ける段階をさらに含み、前記指示情報に含まれる前記操作端末の識別子からこの操作端末に関連付けられた個人情報を抽出し、前記個人情報および前記端末情報からアクセス権を判定する、付記1～7のいずれかに記載の機器制御システムのアクセス制御方法。

【0111】

(付記9)

付記1～8のいずれかに記載の機器制御システムのアクセス制御方法をコンピュータに実行させるためのプログラム。

【0112】

(付記10)

付記9に記載のプログラムを記録したコンピュータ読み取り可能な記録媒体。

(付記11)

有線または無線の宅内ネットワークを介して住宅内の1以上の機器に接続され

、操作端末から送信される前記機器の操作に関する指示信号に基づいて前記機器の制御を行う機器制御サーバであって、

前記操作端末に設定される固有の識別子を前記操作端末のアクセス権と関連付けるための端末情報の登録を受け付ける端末情報受付手段と、

前記端末情報を記憶する端末情報記憶手段と、

前記操作端末の識別子と前記機器の操作に関する指示信号とを含む指示情報を受け付ける指示情報受付手段と、

前記指示情報に基づいて前記操作端末のアクセス権を判定するアクセス権判別手段と、

前記アクセス権判別手段により判定された前記操作端末のアクセス権と前記指示情報に含まれる前記機器の操作に関する指示信号とに基づいて前記機器の制御を行う機器制御手段と、
を含む機器制御サーバ。

【 0 1 1 3 】

(付記 1 2)

前記端末情報の登録を受け付ける際に、前記操作端末に設定される公開鍵を受け付け、前記端末情報とともに前記端末情報記憶手段に格納する公開鍵受付手段と、

所定のデータを送信し、前記操作端末において秘密鍵で暗号化された前記所定のデータを受信し、前記公開鍵により復号化して前記所定のデータと照合することによって、前記操作端末の認証を行う操作端末認証手段と、
をさらに含む付記 1 1 に記載の機器制御サーバ。

【 0 1 1 4 】

(付記 1 3)

電子情報を取得する電子情報取得手段と、

前記電子情報取得手段により取得した電子情報を蓄積する電子情報蓄積手段とをさらに備え、前記機器に関する指示信号が電子情報蓄積手段に蓄積された電子情報へのアクセスを含む場合に、前記アクセス権判定手段は、前記操作端末のアクセス権を判定して前記電子情報の提供を許可するか否かを判断する、付記 1 1

または12に記載の機器制御サーバ。

【0115】

(付記14)

住宅外に存在する宅外ネットワークに接続可能な宅外通信手段をさらに備え、前記機器の操作に関する指示信号が前記宅外ネットワークへのアクセスを含む場合に、前記アクセス権判定手段は、前記操作端末のアクセス権を判定し前記宅外ネットワークへのアクセスを許可するか否かを判断する、付記11～13のいずれかに記載の機器制御サーバ。

【0116】

(付記15)

前記宅外ネットワーク上のコンテンツ毎にアクセスを許可するか否かを判断する、付記14に記載の機器制御サーバ。

【0117】

(付記16)

前記指示情報受付手段により受け付けた指示情報に基づいて、前記操作端末が宅内にあるか宅外にあるかを判別する端末位置判別手段をさらに備え、前記アクセス権判定手段は、前記端末位置判別手段による判別結果に基づいて前記操作端末のアクセス権を判定する、付記11～15のいずれかに記載の機器制御サーバ。

【0118】

(付記17)

前記操作端末を操作するユーザに関する情報を前記操作端末と関連付けるための個人情報の登録を受け付ける個人情報受付手段をさらに含み、前記アクセス権判定手段は、前記指示情報に含まれる前記操作端末の識別子からこの操作端末に関連付けられた個人情報を抽出し、前記個人情報および前記端末情報からアクセス権を判定する、付記11～16のいずれかに記載の機器制御サーバ。

【0119】

(付記18)

住宅内の1以上の機器と有線または無線の宅内ネットワークを介して接続され

る機器制御サーバを有する機器制御システムにおける前記機器の操作に関する指示信号を送信する操作端末であって、

固有の識別子を記憶する識別子記憶手段と、

前記機器制御サーバに前記識別子の登録を行う端末情報登録手段と、

前記機器の操作に関する指示入力を受け付ける入力受付手段と、

前記入力受付手段により受け付けた指示入力と、前記識別子記憶手段に記憶されている識別子とに基づいて指示情報を生成する指示情報生成手段と、

前記指示情報生成手段により生成された指示情報を無線または有線により送信する指示情報送信手段と、

を備える操作端末。

【 0 1 2 0 】

(付記 1 9)

現在の位置情報を取得する位置情報取得手段をさらに備え、

前記指示情報生成手段は、前記指示入力、前記識別子および前記位置情報取得手段により取得した位置情報に基づいて指示情報を生成する付記 1 8 に記載の操作端末。

【 0 1 2 1 】

(付記 2 0)

操作するユーザに関する情報の入力を受け付ける個人情報入力手段をさらに備え、

前記指示情報生成手段は、前記指示入力、前記識別子および前記個人情報入力手段により受け付けたユーザに関する情報に基づいて指示情報を生成する付記 1 8 または 1 9 に記載の操作端末。

【 0 1 2 2 】

(付記 2 1)

秘密鍵を記憶する秘密鍵記憶手段と、

前記秘密鍵に対応する公開鍵を記憶する公開鍵記憶手段と、

前記秘密鍵によりデータを暗号化する暗号化処理手段と、

をさらに含み、前記端末情報登録手段により前記機器制御サーバに端末情報の登

録を行う際に前記公開鍵を前記機器制御サーバに送信し、前記指示情報を送信する際に、前記機器制御サーバから受信する所定のデータを前記秘密鍵によって暗号化して認証情報として送信する、付記 1 8 ～ 2 0 のいずれかに記載の操作端末。

【 0 1 2 3 】

【発明の効果】

本発明によれば、機器制御サーバへのアクセス権を操作端末毎に設定して操作端末の識別子に関連付けて登録しているため、宅内からアクセスに対しても宅外からのアクセスに対しても、機器の操作に関する指示情報を受け付けることが可能となり、第 3 者による不正なアクセスを防止するとともに、操作端末毎のパスワードや利用する情報毎のパスワードの設定やこれを記憶する手間を省略することができる。

【図面の簡単な説明】

【図 1】

本発明の概略構成を示す説明図。

【図 2】

機器制御サーバの概略構成を示すブロック図。

【図 3】

操作端末の概略構成を示すブロック図。

【図 4】

機器制御サーバにおける登録受付処理を示すフローチャート。

【図 5】

操作端末における登録処理を示すフローチャート。

【図 6】

機器制御サーバにおける端末認証処理を示すフローチャート。

【図 7】

端末認証処理時の操作端末の動作を示すフローチャート。

【図 8】

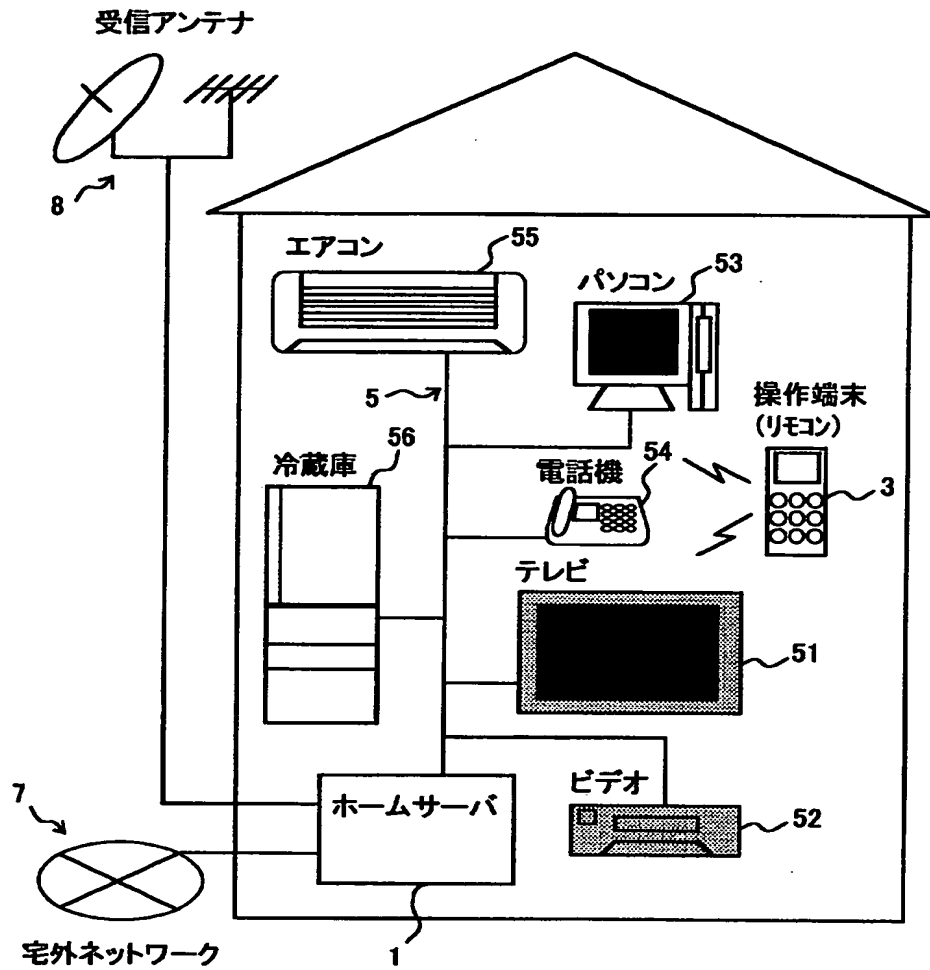
個人情報登録処理を示すフローチャート。

【図 9】

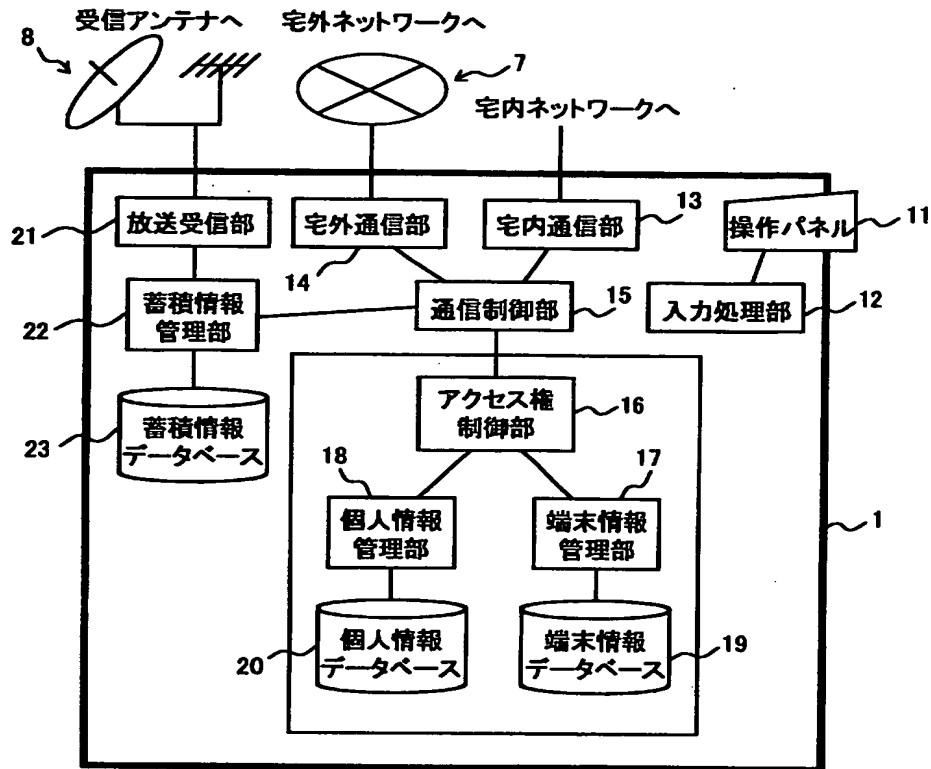
端末情報と個人情報とを用いたアクセス制限の処理を示すフローチャート。

【書類名】 図面

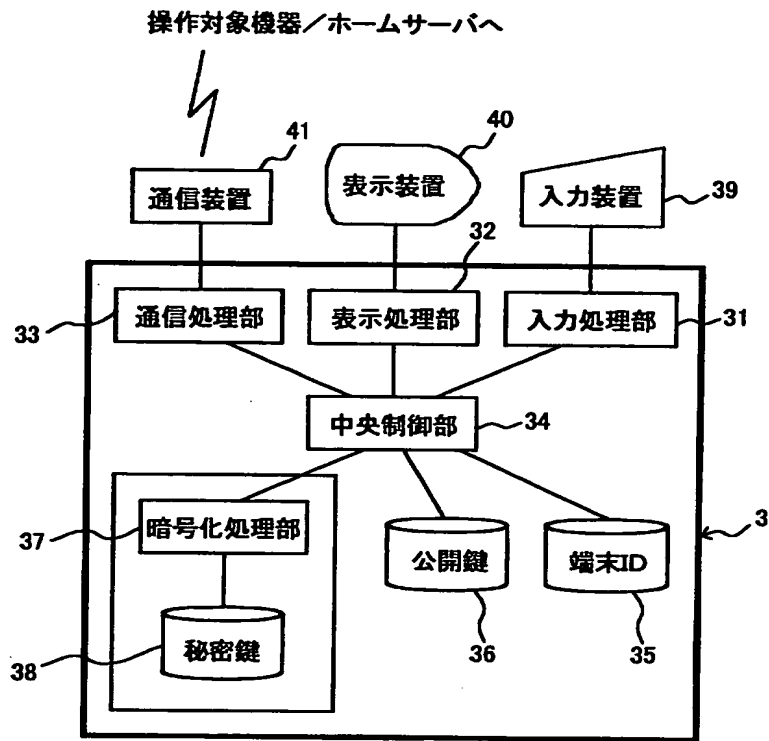
【図1】



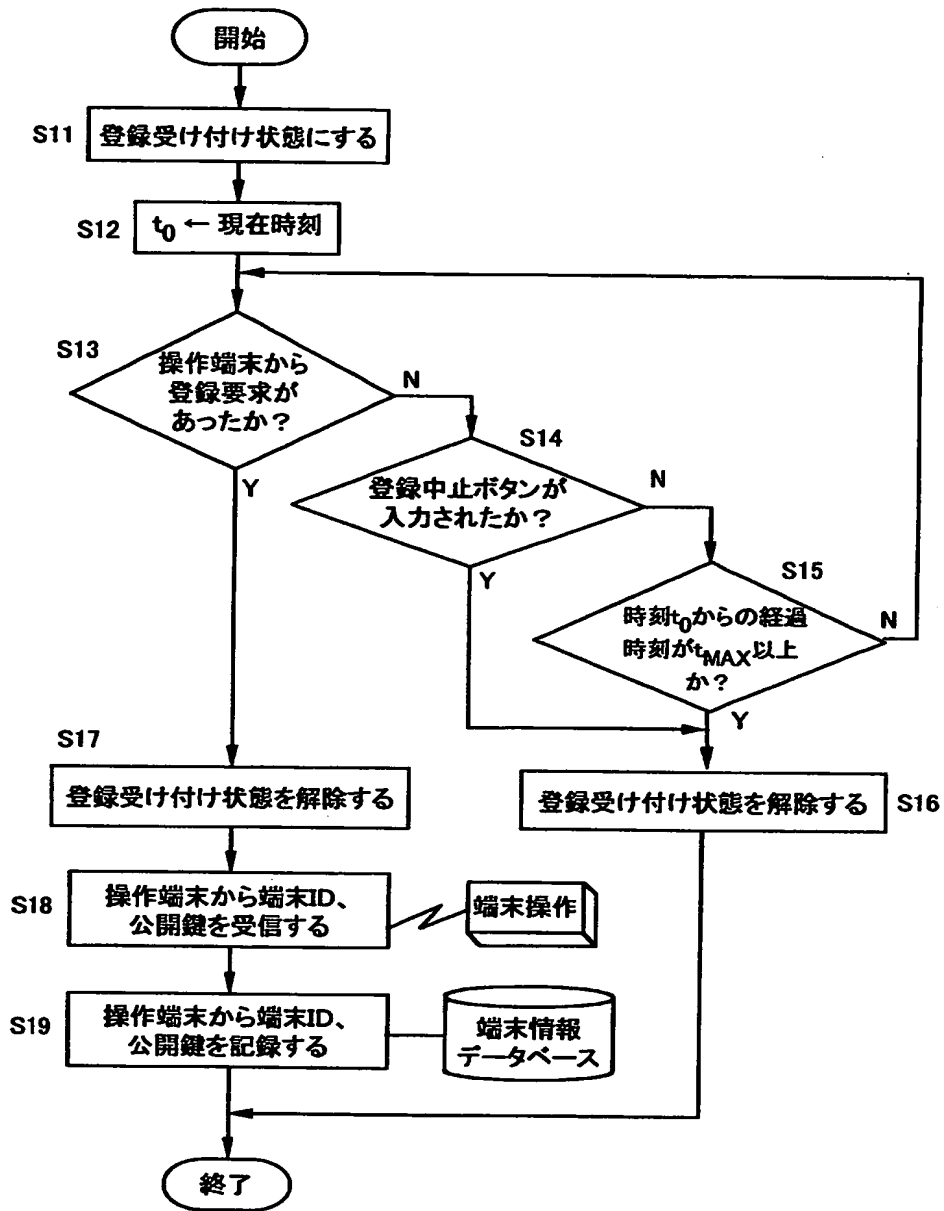
【図2】



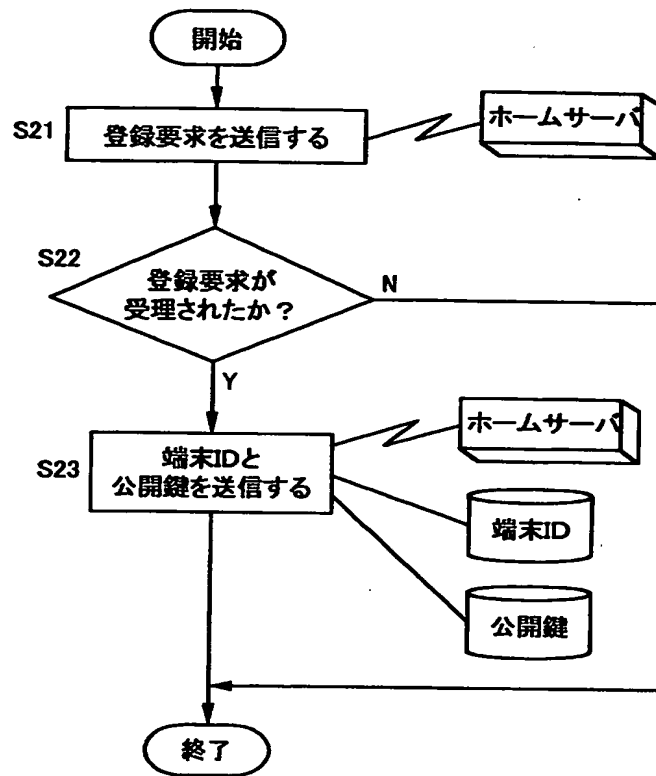
【図 3】



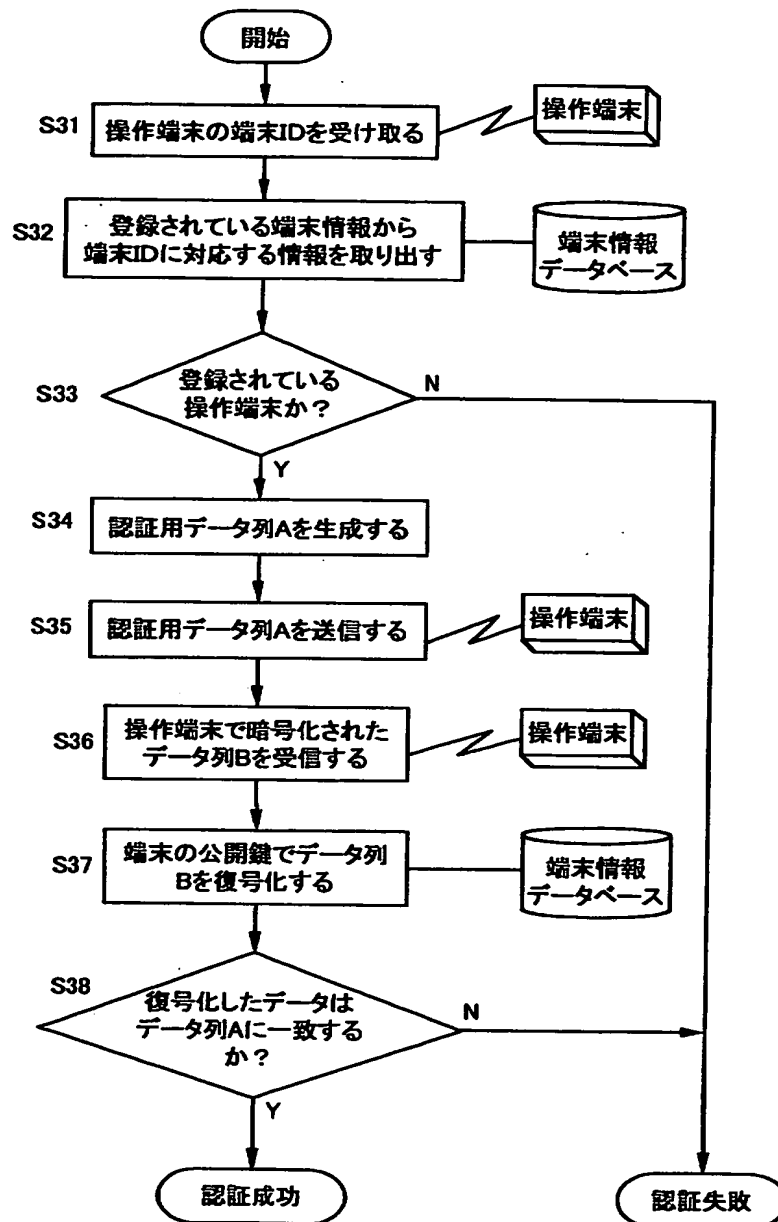
【図 4】



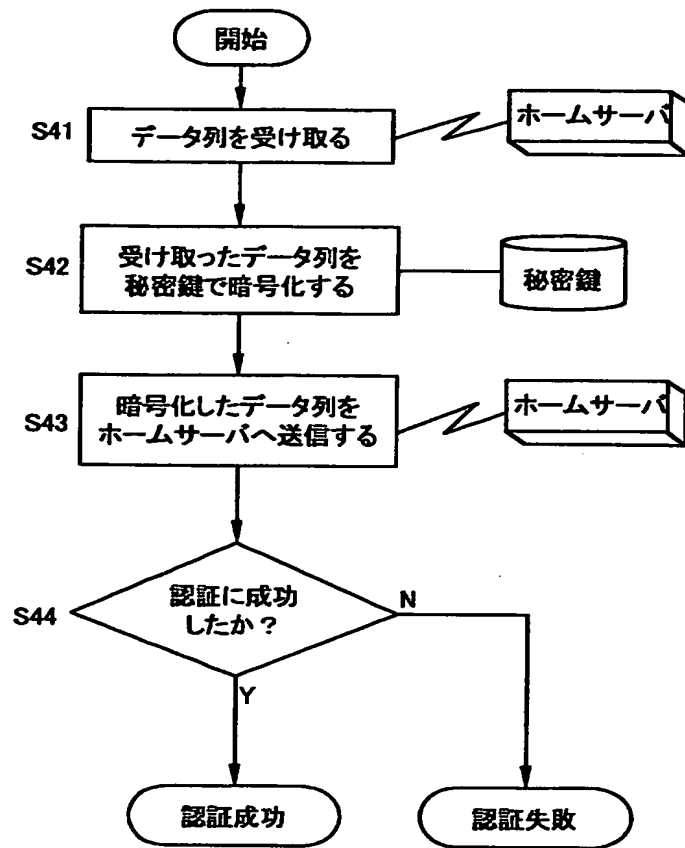
【図5】



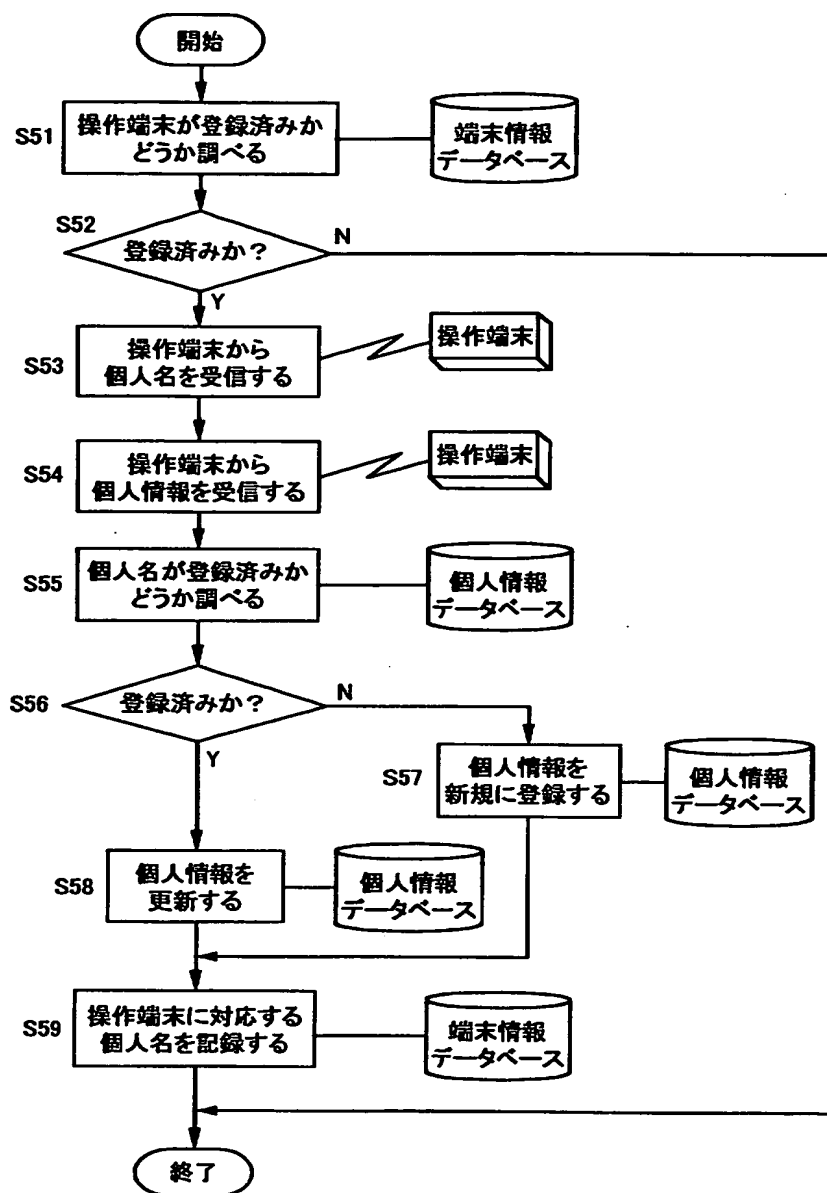
【図6】



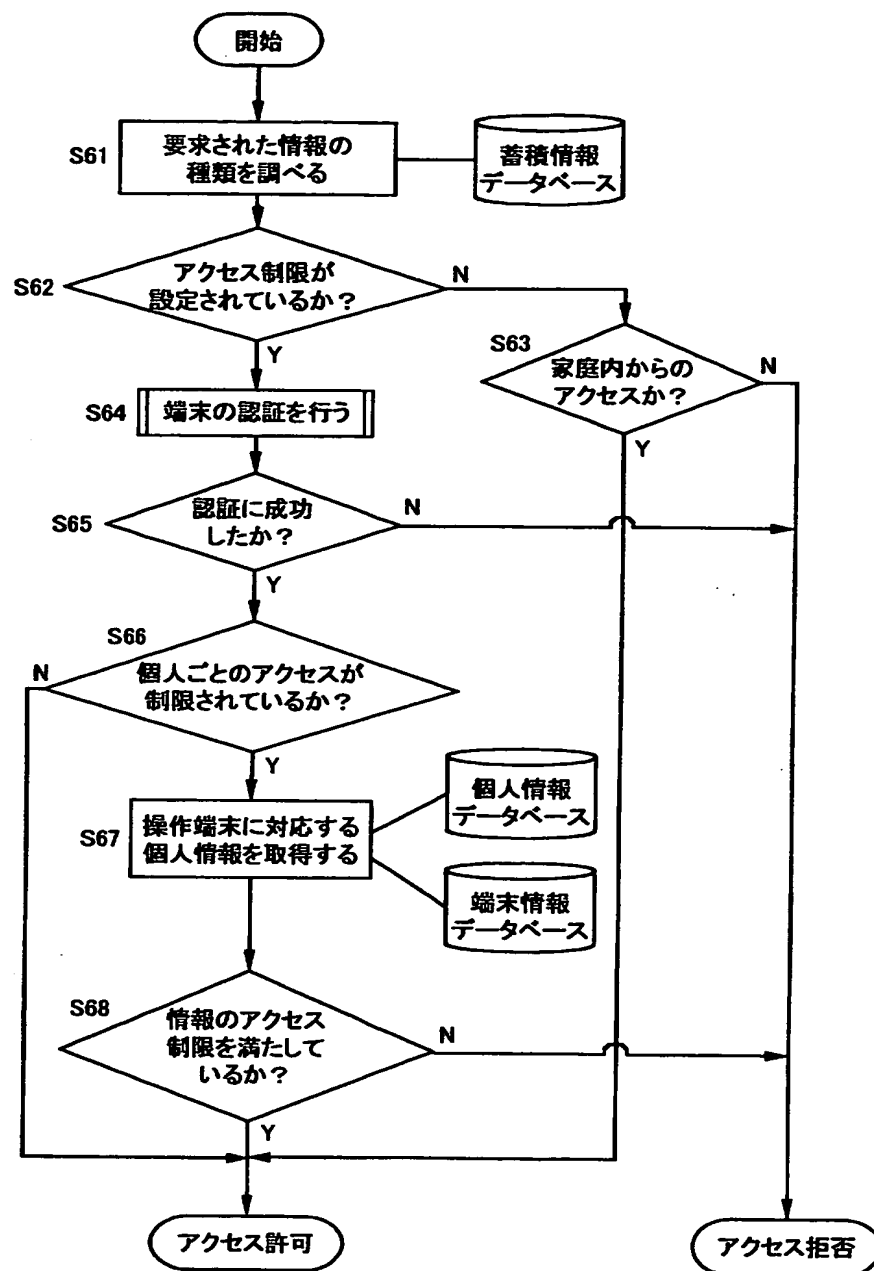
【図 7】



【図 8】



【図 9】



【書類名】 要約書

【要約】

【課題】 住宅内の機器を制御する機器制御システムにおいて、利用者の認証作業の手間を軽減するとともに、第 3 者からの不正なアクセスを防止する。

【解決手段】 操作端末に設定される固有の識別子を操作端末のアクセス権と関連付けるための端末情報の登録を受け付ける段階と、操作端末の識別子と機器の操作に関する指示信号とを含む指示情報を受け付ける段階と、指示情報に含まれる操作端末の識別子から操作端末のアクセス権を判定する段階と、操作端末のアクセス権と機器に関する指示信号とに基づいて前記機器の制御を行う段階とを含む機器制御システムのアクセス制御方法。

【選択図】 図 2

出 願 人 履 歴 情 報

識別番号 [000005223]

1. 変更年月日 1996年 3月26日

[変更理由] 住所変更

住 所 神奈川県川崎市中原区上小田中4丁目1番1号
氏 名 富士通株式会社